La publicación abre el debate a la discusión, análisis y reflexión sobre el llamado derecho al olvido y los desafíos éticos que plantea el escenario mediático digital a la luz de nuevos hallazgos y posibilidades de interpretación. Las recientes innovaciones tecnológicas en las comunicaciones digitales han aumentado la importancia de resolver problemas de privacidad y libre expresión.

El derecho al olvido ha recibido cierto apoyo de los estudiosos de los Estados Unidos, aunque generalmente es mal visto debido a conflictos potenciales con las protecciones a la libre expresión de la Primera Enmienda a la Constitución. Sin embargo, los Estados Unidos tienen algunos aspectos del derecho al olvido como la reciente Ley de Borrado en Línea, de California, para adolescentes. También tiene una larga historia de tribunales que protegen el derecho de las personas a cambiar sus vidas, se perdonan las transgresiones pasadas y dejan atrás el pasado cuando ya no es noticia.

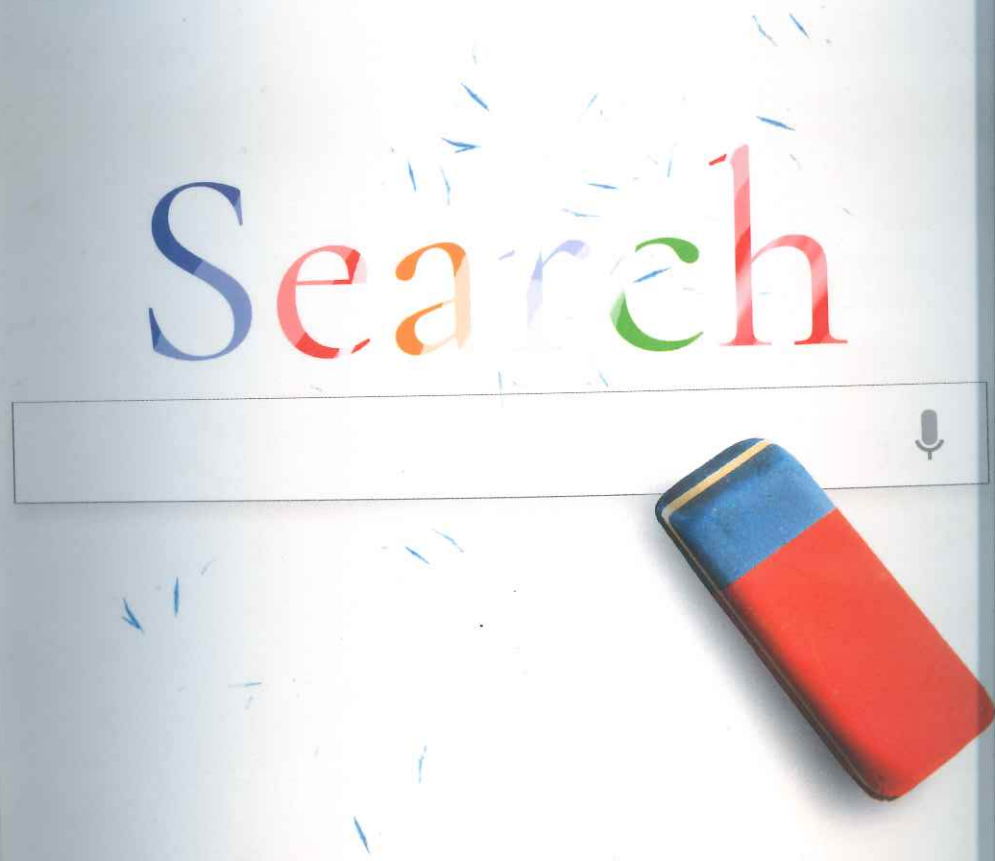
La dimensión ética analizada, reviste fundamental importancia en un escenario mediático digital en el que las audiencias han tomado la palabra, auditan, escrutan, analizan y desean participar en los contenidos de los medios, reclaman derechos como el de réplica o de rectificación y los concernientes al ejercicio profesional en los medios. Lo anterior no sólo pone en cuestión y admite una revisión en la industria, sino también la manera de ejercer el periodismo. La apuesta por la aplicación de dichos sistemas debería ser un objetivo *a priori*, perseguido por toda empresa de comunicación y multimedia ya que la credibilidad de cualquier contenido agrega valor al medio.

ISBN 978-956-01-0517-2
9 789560 105172

UNIVERSIDAD MAYOR

MARÍA JOSÉ LABRADOR • EDWARD CARTER [COORDS.]
GOOGLE: DERECHO AL OLVIDO Y DESAFÍOS ÉTICOS EN EL ESCENARIO MEDIÁTICO DIGITAL

GOOGLE: DERECHO AL OLVIDO Y DESAFÍOS ÉTICOS EN EL ESCENARIO MEDIÁTICO DIGITAL



MARÍA JOSÉ LABRADOR
EDWARD CARTER
[COORDS.]

UNIVERSIDAD MAYOR

RIL editores

323.445 Labrador Blanes, María José
L Google: derecho al olvido y desafíos éticos en el escenario mediático digital / Coordinadodres: María José Labrador Blanes, Edward Carter . – – Santiago : RIL editores - Universidad Mayor, 2017.

230 p. ; 23 cm.
ISBN: 978-956-01-0517-2

1 GOOGLE (FIRMA COMERCIAL : ESTADOS UNIDOS). 2 REDES SOCIALES-ASPECTOS JURÍDICOS. 3 SITIOS WEB-ASPECTOS POLÍTICOS.

GOOGLE: DERECHO AL OLVIDO Y
DESAFÍOS ÉTICOS EN EL ESCENARIO MEDIÁTICO DIGITAL
Primera edición: enero de 2018

SEDE SANTIAGO:
Los Leones 2258
CP 7511055 Providencia
Santiago de Chile
(56) 22 22 38 100
ril@rileditores.com • www.rileditores.com

SEDE VALPARAÍSO:
Cochrane 639, of. 92
CP 2361801 Valparaíso
(56) 32 274 6203
valparaiso@rileditores.com

SEDE ESPAÑA:
europa@rileditores.com • Barcelona

Composición e impresión: RIL® editores
Diseño de portada: Matías González Pereira

Impreso en Chile • *Printed in Chile*

ISBN 978-956-01-0517-2

ÍNDICE

Todo esto y mucho más se podía pedir a nuestros legisladores, con la casi certeza de que, si se me permite, esta *carta a los Reyes*, caerá en saco roto. Me atrevo a compartir cierta desesperanza respecto de la adecuación del Derecho a las nuevas, y no tan nuevas, tecnologías que con gran acierto Rodríguez ha verbalizado:

> En la medida en que cada vez mayor número de ciudadanos acudirán a internet para confiarle más y más facetas de su existencia, estos problemas no harán sino incrementarse y resultar más patentes.
>
> Por otra parte, todo parece indicar que en una buena porción de importantes cuestiones el ciberespacio y el Derecho seguirán sus respectivas órbitas tranquilamente, desconocidos el uno para el otro. Puede que de modo eventual esas 'órbitas' se alineen en algún punto, pero esto no será lo frecuente. [...] La rápida evolución de internet contrasta con la lentísima evolución de la creación del derecho, y nada hace pensar que ambos rasgos vayan a cambiar[56].

[56] Rodríguez García, Luis Fernando, «Políticas de la Federal Communications Commission en materia de neutralidad de la red», en Cotino Hueso, L. (editor), *Libertades de expresión e información en Internet... cit.* pp., 99-113.

El derecho al olvido en internet y el efecto Streisand: aplicabilidad y soluciones

Óscar Jaramillo
Lucía Castellón

Pese a que el Tribunal de Justicia de la Unión Europea le ordenó a Google borrar de su base de datos la dirección de una página *web* en la que se anunciaba el remate de bienes de un ciudadano español, hoy es posible encontrar más siete mil resultados sobre esta persona y lo que es más interesante, la página que supuestamente se debía borrar. Esta ponencia aborda desde el punto de vista de la ciberética, las razones por las cuales ello sucede y explora la aplicabilidad del derecho al olvido en los distintos ecosistemas digitales: la web 1.0, 2.0 y 3.0.

La tesis central es que, tanto desde el punto de vista técnico como ético, la aplicación del derecho al olvido varía en cuanto a sus motivos, funciones y posibilidades de aplicación, si se trata de eliminar contenidos de sitios *web*, redes sociales, aplicaciones o estamos frente al fenómeno del big data. A partir de la ya clásica afirmación de Lessig (2006) de que el código es ley, vemos el enfrentamiento de dos arquitecturas de red básicas: la del control y la libertad. Ambas se ven enfrentadas en los distintos ecosistemas digitales al punto de configurar soluciones y problemas al momento de aplicar el derecho al olvido en internet.

El primer caso de derecho al olvido y el efecto Streisand

De ser una persona común y corriente, Mario Costeja pasó a ser una verdadera celebridad en línea, cuando el Tribunal de Justicia de la Unión Europea emitió el falló en el que obligó a Google a borrar desde su base de datos, una página del diario *La Vanguardia* en la cual se anunciaba el remate de sus bienes.

Su intención era que cada vez que alguien buscara su nombre en Google, no apareciera el enlace hacia una página del diario *La Vanguardia* del 19 de enero de 1998, en la cual se anunciaba el remate de sus bienes por deudas impagas. El anuncio era pequeño, de cuatro líneas, abajo, en una ubicación casi imperceptible.

El problema es que el efecto que produjo el fallo del Tribunal de Justicia de la Unión Europea, en el que se reconoce el derecho al olvido de este ciudadano español, fue absolutamente contrario a lo que se buscaba. Basta con colocar Mario Costeja en Google, para que de inmediato se desplieguen 45 mil 900 resultados. Y si realizamos una nueva búsqueda en la cual ingresemos el término de búsqueda «Mario Costeja La Vanguardia», de inmediato aparecerán 7 mil 740 resultados, entre los que destacará el primero: el hipervínculo hacia la página que originalmente Google debía borrar desde su base de datos.

Dentro del ecosistema digital, esto es lo que se conoce como el efecto Streisand. Este concepto se aplica a los casos en los cuales una orden judicial que intenta censurar en internet una información que pasó desapercibida para los medios de comunicación y la opinión pública se viraliza después gracias a la prohibición.

¿Por qué sucede esto? ¿Por qué este ciudadano español pasó de tener un enlace a una página en PDF en donde su nombre aparecía en un lugar casi imperceptible, a tener más de cuarenta mil resultados con fotografías que se despliegan de manera automática? ¿Y por qué aún es posible acceder desde Google a la página que el Tribunal de Justicia de la Unión Europea ordenó eliminar de su base de datos?

Tal como lo señala Ausloos (2012), el derecho al olvido debe ser definido de mejor manera para evitar consecuencias negativas. De lo contrario, su aplicación producirá el efecto contrario. Para que ello no ocurra, es necesario tener una mayor comprensión del ecosistema de medios digitales, más allá de achacar la responsabilidad a los motores de búsqueda como Google.

Si lo que buscamos es que las personas puedan aplicar el derecho al olvido sin que se produzca el efecto Streisand, es necesario comprender lo que Jenkins (2007) denomina como la cultura de la convergencia y que no es otra cosa que la intersección entre la comunicación y la tecnología, con todas las implicaciones culturales que ello conlleva.

Posibilidades de aplicación del derecho al olvido

Nuestra hipótesis es que es sumamente complejo aplicar el derecho al olvido si previamente no se entiende el funcionamiento del ecosistema digital, comprendido este en sus vertientes tecnológica, cultural y comunicacional. Nuestro punto de partida serán las arquitecturas de red, por sus efectos en las costumbres y usos de las comunidades en línea, junto con el desarrollo tecnológico y comercial que ha tenido el universo digital. Con posterioridad nos centraremos en el fenómeno del big data, por las implicancias que tiene en la vida privada de las personas y en las lógicas de recopilación,

almacenamiento y procesamiento de información personal. Una vez que analicemos este problema, nos centraremos en el funcionamiento de las redes sociales y motores de búsqueda, debido a que gran parte de la aplicación del derecho al olvido depende de la forma en que se publica, etiqueta, comparte e indexa la información.

La diferencia entre una aplicación efectiva del derecho al olvido que evite la revictimización y el efecto Streisand, depende de una definición adecuada de este derecho, que contemple las costumbres, la forma de comunicarse y la tecnología.

Arquitecturas de red

«El código es ley». Esa es una de las afirmaciones clásicas de Lessig (2006) para señalar que tanto el *software* como el *hardware* son básicos para definir el funcionamiento y las costumbres que se producen al interior de los entornos digitales. Tal como lo señala McLuhan (1962), el hombre creó la tecnología y la tecnología moldeó al hombre.

La idea que hay detrás de lo anterior es que para comprender las costumbres y culturas que se dan al interior de los entornos digitales, primero hay que descifrar el funcionamiento de la tecnología, al nivel más básico que es el de la programación, ya que ella regularía nuestro comportamiento. Una pista básica es la que da Lessig al señalar que el código, entendido como la conjunción de *software* y *hardware*, define las posibilidades que tienen las personas para actuar en su vida cotidiana.

Un ejemplo de ello es el que da Boyd (2014) al señalar que los adolescentes norteamericanos utilizan las redes sociales para compartir con sus pares, debido a los problemas de desplazamiento y tráfico propios de las urbes modernas. Debido a la imposibilidad de juntarse y compartir presencialmente, deben realizarlo de forma virtual. Según Boyd, esa imposibilidad de mantener un contacto físico de manera fluida genera la costumbre propia de los adolescentes de estar constantemente chateando a través de los teléfonos inteligentes.

Para entender las lógicas propias de las tecnologías digitales y cómo ellas influyen en las costumbres de las personas, hay que analizar lo que Lessig (2006) define como la arquitectura de red. Cuando hablamos de la arquitectura de red, nos estamos refiriendo al diseño básico de internet y, por añadidura, a las TIC (tecnologías de la información y la comunicación).

Tal como lo señalan Lessig (2006) y Castells (2012), la primera arquitectura de internet fue diseñada por investigadores y *hackers*; mientras que la segunda, por el sector comercial. La característica central del diseño inicial de la red fue el anonimato, el cual se garantizó a través de una característica básica: la utilización de un diseño en red, en el cual cada nodo tiene la potencialidad de comunicarse con cualquier otro. En términos sencillos, eso significa que carece de un nodo central, que controle y regule todo lo que pasa a través de la red.

Si volvemos al tema del derecho del autor y la forma en que el Tribunal de Justicia de la Unión Europea ha tratado de resolver el problema, esto marca una de las principales dificultades para que ello ocurra. Debido a que internet tiene una arquitectura reticular, la única condición que debe cumplir un nodo para sumarse a la red es respetar el protocolo de comunicación TCP/IP.

En la práctica, eso implica que la publicación de información en internet no puede ser controlada. Para publicar información, el servidor solo debe cumplir con utilizar el mismo lenguaje de comunicación. Desde el punto de vista del derecho al olvido, eso implica que no se puede impedir que alguien publique información, ni tampoco se puede borrar por algún ente central. Asimismo, cualquier persona o entidad puede crear aplicaciones que funcionen en la *web*, siempre y cuando respete los protocolos de comunicación.

Eso significa que, si un tribunal de justicia ordena borrar un archivo, solo puede hacerlo el autor o el responsable del servidor. Pero lo que es más importante el hecho de que un tribunal de justicia ordene borrar un archivo desde un servidor, no implica que distintas personas suban copias de ese contenido a distintos servidores, para que esa información siga disponible. Esa es razón por la que en la actualidad Mario Coteja tiene miles de resultados más de los que preocuparse,

que antes de que el Tribunal de Justicia de la Unión Europea acogiera su solicitud en la que reclamaba su derecho al olvido.

En tanto, la arquitectura de red diseñada por el sector comercial se basó en la identificación de las personas, al contrario del diseño anterior. El impulso del comercio electrónico y de procesos gubernamentales hizo necesario que se requiriera identificar a las personas cuando se encontraban en internet.

Como resultado de esta nueva arquitectura de red en la cual es posible identificar a una persona a través del rastreo de los números IP, se crea lo que Lessig (2006) denomina como una falsa sensación de anonimato en línea. Según este autor, la única forma de anonimato que queda en la actualidad es utilizar un teléfono inteligente prepagado.

A las personas que no están familiarizadas con la métrica *web* (Kaushik, 2010), les puede parecer un tanto extraño que el *web master* de cualquier sitio sepa la ubicación geográfica y la segmentación etaria y por género de los visitantes de una página. El hecho de que sea posible identificar a las personas en los entornos digitales ha tenido como resultado la baja en la utilización de *software* pirata. De hecho, la única forma en la actualidad de utilizar un programa de manera ilegal, es a través de *hacks* que bloquean el envío de información al servidor de la empresa propietaria del *software*, de la identidad del dueño del computador.

Aplicaciones como Google Analytics le permiten a los *webmaster* identificar una serie de parámetros propios del dispositivo y las personas que visitan un sitio. A través del uso de *cookies*, *super* y *über cookies*, es posible identificar el sistema operativo, el navegador, resolución de pantalla, antivirus y hasta los programas cargados en el dispositivo.

Y tal como lo dijimos anteriormente, es posible identificar el género, edad y ubicación de nuestros visitantes, gracias al rastreo del número IP. La IP es un número de identificación único, que forma parte del ADN de internet, porque es necesario para que cualquier dispositivo se conecte a la red.

En los inicios de internet, las IP se asignaban de manera dinámica para garantizar el anonimato. Eso significa que, al momento de conectarse a internet, el servidor le asignaba de manera automática una IP a

ese computador, que se mantenía por el tiempo que durara la conexión. Cuando se volviera a ingresar a internet, se le asignaba una nueva IP, lo cual garantizaba el anonimato de esa persona.

Lessig (2006) señala que la necesidad de un mayor control en internet para garantizar el comercio en línea hizo que fuera necesario identificar a las personas. La forma de hacerlo fue la asignaciónn de IP únicas. Es decir, para que un dispositivo se pudiera conectar a internet, se le entregó una IP que se mantiene a través del tiempo.

La forma de relacionar una IP con el nombre de una persona es más sencillo de lo que se puede pensar. Además, los mecanismos son variados y van desde soluciones de baja a alta tecnología y pasan por distintos grados de intrusión. Lo más básico es el registro de los sistemas operativos al configurar por primera vez un computador, tableta o teléfono inteligente. Al iniciar el dispositivo es necesario conectarlo a internet, para después crear una cuenta en Microsoft, Apple o Google, en el caso de que se trate de un dispositivo móvil con Android. Al generar la cuenta se colocan datos sensibles como el nombre, edad, género, dirección, correo electrónico y número de teléfono. Lo mismo sucede con la mayor parte de las aplicaciones actuales, las cuales requieren que los usuarios creen una cuenta para utilizar el programa. De esa manera, se relaciona la IP al nombre de una persona específica. Asimismo, la condición básica para utilizar el *software* es estar *logueado*. Es decir, con una sesión abierta que permite que el servidor del *software* reconozca y registre todo lo que la persona está realizando.

A esto hay que sumar la práctica de numerosos sitios que registran a sus usuarios para acceder a contenidos especiales o realizar compras o trámites en línea. Al registrarse, se puede asociar la IP con el nombre de una persona. Además, se puede enviar una *cookie* o troyano al disco del dispositivo, para reconocerlo cuando el usuario regrese al sitio sin registrarse o *loguearse*, tal como habitualmente se dice en los entornos en línea.

Por otra parte, es necesario señalar que existen mecanismo de corte intrusivo para leer el registro del sistema operativo, lo que permite identificar a un usuario sin necesidad de que este se registre.

Existen todo tipo de *worms* (gusanos) o troyanos que se instalan en el disco del dispositivo y tienen la capacidad de leer el registro del sistema operativo o el teclado para determinar la identidad del usuario. Y cada vez que esa persona se conecte a internet, envían un informe de actividades al servidor de la entidad que los creó.

Un punto que es necesario aclarar es que ambas arquitecturas coexisten en internet, tanto desde el punto de vista tecnológico como cultural. Eso significa que el anonimato y el monitoreo de todas las actividades en el mundo real y virtual están al alcance de la mano, para todas aquellas personas e instituciones que tengan los recursos y los conocimientos técnicos.

Mientras que el anonimato en la red va de la mano con la cultura *hacker*, la identificación de los usuarios está directamente relacionada con el comercio. Eso significa que a través del uso de servidores proxis y programas creados y mantenidos por grupos de *hackers*, es posible navegar y subir contenido a internet de manera absolutamente anónima. Y al mismo tiempo, la industria tecnológica puede mantener un monitoreo en tiempo real de todas las actividades virtuales y reales de los usuarios. En el año 2011, Apple reconoció que el iPhone registraba todos los lugares en los que habían estado sus usuarios a través del uso del GPS y que esa información se enviaba a sus servidores (Emol, 2011).

Por lo tanto, el anonimato es posible únicamente para las personas con un alto grado de conocimiento técnico, ligado a la cultura *hacker*. Y la identificación solo la pueden lograr empresas y organizaciones con acceso a *data centers* y servicios de programación altamente especializados. El usuario común y corriente solamente tiene la ilusión del anonimato, mientras que cada una de sus acciones es monitoreada, registrada, almacenada y procesada, sin darse cuenta de ello, por la industria tecnológica y *hackers*.

Desde la internet 1.0 a la 3.0

Hemos llegado al punto central de lo que Jenkins ha denominado como la cultura de la convergencia, en donde ambas arquitecturas

—las que abogan por el anonimato y la identificación en línea— se ven enfrentadas.

Para poder entender el derecho al olvido en el ecosistema digital, es necesario hacer la diferenciación entre lo que Payton y Claypoole (2014) denominan como internet 1.0, 2.0 y 3.0, ya que es allí donde las diferentes arquitecturas de control toman fuerza. Desde un punto de vista tecnológico, la aplicación del derecho al olvido adquiere distintos objetos y finalidades en cada uno de los estratos que hemos definido. Por lo mismo, su posible aplicación tiene distintas finalidades y posibilidades de aplicación, desde el punto de vista técnico.

La internet 1.0 es lo que habitualmente conocemos como la *web*, en donde los contenidos son publicados en sitios y *blogs*. Pese a que la mayor parte de los sitios actuales cuentan con la posibilidad de «postear» comentarios, la *web* 1.0 se caracteriza por tener un tipo de comunicación más bien lineal y por poseer contenidos de corte estático, que son publicados por profesionales o semiprofesionales (blogueros) de la comunicación.

En cambio, lo 2.0 está eminentemente asociado a las redes sociales, lo que implica que son los propios usuarios quienes crean los contenidos. A diferencia de la *web* 1.0, el principal mecanismo de difusión es la viralización, en el cual los contenidos son compartidos por las personas. Esto tiene grandes implicancias para la aplicación del derecho al olvido, porque al viralizarse un contenido, significa que el archivo es copiado en el dispositivo y subido a la nube por cada persona que lo comparte. Eso implica que para aplicar el derecho al olvido habría que borrar el archivo en cada tableta, teléfono inteligente o computador de cada uno de los usuarios que lo compartió. Eso sin tomar en cuenta que, por defecto, cada archivo almacenado en el disco duro se copia de manera automática en la nube.

Cabe señalar que el concepto de nube no lo hemos utilizado al azar, ya que está directamente relacionado con el siguiente nivel: 3.0. Habitualmente, el concepto de internet 3.0 se relaciona con la inteligencia artificial, la internet de las cosas y la *web* semántica, lo cual nos lleva al plano de los datos y los metadatos. En la práctica

lo que configura es el fenómeno del big data, que es necesario para comprender el alcance que tiene la recopilación de datos personales en el ecosistema digital y la necesidad de implementar el derecho al olvido.

Según Needham (2014), el big data es un tipo de supercomputación para empresas comerciales y gobiernos que hace posible monitorear una pandemia apenas ocurre, anticipar dónde sucederá el próximo asalto bancario, optimizar la cadena de suministros de la industria de comida rápida, predecir el comportamiento de voto el día de elecciones y pronosticar los levantamientos políticos al mismo momento en que están ocurriendo.

En términos sencillos, es necesario comprender que cada actividad desarrollada a través de un aparato digital produce un metadato (dato del dato), que indica quién, cuándo, cómo y dónde realizó esa acción. El big data consiste en registrar esos metadatos —junto con los datos—, almacenarlos y procesarlos para realizar perfiles de usuarios y, de esa manera, predecir su conducta. Cabe señalar que los datos utilizados para realizar big data provienen de los sensores (GPS, cámara, acelerómetros y micrófonos) de teléfonos inteligentes, vestibles (Google Glass o relojes inteligentes), tabletas, automóviles y hasta de cámaras de seguridad. A ello hay que sumar todos los datos que se obtienen gracias al uso de las tarjetas de crédito y débito, además del registro de la navegación por internet y el uso de las redes sociales. Si consideramos que las últimas versiones de OSX y Android poseen aplicaciones que al conectarse con los sensores de vestibles permiten registrar el pulso, frecuencia cardiaca, temperatura y otros parámetros corporales, el big data lleva el derecho al olvido a un plano desconocido, en donde es posible anticipar no solo el comportamiento, sino que los estados de salud de las personas.

La internet 3.0 y el big data nos llevan a un nuevo nivel que tiene dos dimensiones básicas, si queremos analizar el tema del derecho al olvido: el almacenamiento de toda la información proveniente de la internet 1.0 y 2.0, junto al registro de los metadatos asociados (1.0 y 2.0). Lo 3.0 lleva la indexación de contenidos a un nivel superior a lo realizado por los buscadores tradicionales, como Google o Bing.

Cuando hablamos de big data, nos estamos refiriendo al almacenamiento de toda la información y metadatos provenientes de la *web*, las redes sociales, vestibles y aparatos digitales que tenga sensores. En este punto debemos ampliar el concepto de dispositivos a aparatos, para poder incluir automóviles, electrodomésticos y edificios inteligentes. Y a ellos hay que sumar todos los datos y metadatos que están en la nube.

Las implicancias que esto tiene para la aplicación del derecho al olvido son numerosas, y para entenderlas, es necesario que nos detengamos brevemente en el concepto de nube. Toda la información que está en la *web* 1.0 debe ser previamente subida a un servidor de contenidos (*hosting*) que tiene parámetros profesionales y comerciales. Eso significa que para poder publicar algo en la *web*, previamente debemos contratar un servidor o crear uno propio, lo cual requiere de grandes conocimientos técnicos. En la práctica, eso implica un mayor nivel de control porque el proceso de publicación de contenidos tiene un carácter más bien profesional, tanto desde el punto de vista periodístico como técnico.

Al contrario, la nube es una especie de *web* personal, a la cual podemos acceder desde cualquiera de nuestros dispositivos. Allí podemos mantener una copia de nuestros correos electrónicos, videos, fotografías o documentos para poder acceder a ellos desde el computador, teléfono inteligente o *tablet*. La mayor parte de los dispositivos móviles basados en Android y OSX copian por defecto todos los archivos que reciben o que se creen con ellos, a la nube. La diferencia fundamental entre un servidor de alojamiento (*hosting*) de páginas *web* y la nube, es la facilidad de uso y la automatización de los procesos.

Para ejemplificarlo, el servicio de libros electrónicos Kindle. Amazon vende tabletas cuya pantalla tiene la tecnología de papel digital, desde la cual se pueden leer y comprar libros electrónicos. Sin embargo, desde la *web* y mercado de aplicaciones de Apple y Android (Google) se pueden descargar aplicaciones que permiten instalar el *software* de Kindle en computadores, teléfonos inteligentes y tabletas. Estas aplicaciones funcionan bajo el concepto de nube, por lo que es posible leer un libro en el dispositivo electrónico de

Amazon y apagarlo, para continuar la lectura en el computador. Al abrir la aplicación, el computador se conectará con la nube para abrir el libro en la misma página que se había dejado en el *e-book*. Para que esto ocurra, la aplicación reproduce los datos (el libro) y los metadatos (la página) en la nube, para que se pueda acceder a ellos desde otro dispositivo.

Las implicancias que esto tiene para el derecho al olvido son importantes porque si se quisiera borrar una fotografía vergonzosa, habría que eliminarla desde cada dispositivo y nube asociado a ello. Cabe señalar que desde el punto de vista técnico eso es posible, pero el mecanismo para realizarlo es altamente intrusivo.

Tal como lo explican Craig y Ludloff (2011), Amazon borró de los Kindles (dispositivo de lectura) de sus usuarios *Animal Farm* y *1984* de Orwell. Para ello utilizó la tecnología TPM (*Trusted Platform Module*), más conocida como Fritz Chip, que fue desarrollada originalmente para evitar el pirateo de música y programas computacionales en computadores. El TPM es un chip que está en la totalidad de los computadores actuales y la gran mayoría de los teléfonos inteligentes y tabletas, que permite acceder de manera remota a un dispositivo digital que contenga material que no respeta los derecho de autor y eliminarlo o bloquearlo, para que no pueda ser utilizado. Si bien es cierto que el TPM podría ser utilizado para hacer efectivo el derecho al olvido, quedan dudas de lo ético que puede ser acceder de manera remota a un dispositivo digital y borra archivos en él. Asimismo, crea el campo fértil para ejercer la censura en una infinidad de campos, a un nivel nunca antes visto.

Cabe señalar que el big data y el tipo de comportamiento que hemos explicado anteriormente están restringidos a empresas y organizaciones gubernamentales, debido a que se necesita acceso a servidores, *software* y personal calificado para realizar el almacenamiento y procesamiento de la información.

Como podemos observar, la nube permite comportamientos dicotómicos en los que las arquitecturas de la libertad y el control se dan al mismo tiempo de manera casi simultánea.

A partir de lo que hemos analizado anteriormente, queda claro que es muy distinto hablar del derecho al olvido en los entornos 1.0, 2.0 y 3.0. Esa es la razón por la cual, antes de ver posibles soluciones (si es que las hay), debemos configurar las razones y aplicaciones del derecho al olvido en cada uno de dichos ecosistemas digitales. En lo que hemos denominado como el ecosistema 1.0, es donde sucedió el caso de Mario Costeja y, claramente, la solución el Tribunal de Justicia de la Unión Europea no fue la más apropiada. Tal como lo hemos dicho anteriormente, en este caso el problema se produjo por la publicación de un aviso en la página *web* de un diario electrónico. Lo que les llama la atención a muchos es que la resolución del Tribunal de Justicia de la Unión Europea solo se aplicara a Google. El primer aspecto que hay que tener en cuenta, es que para ejercer el derecho al olvido de manera efectiva en la *web* 1.0 es necesario considerar la subida de archivos a los servidores de alojamiento (*host*) y el proceso de indexación de contenidos por parte de los motores de búsqueda. Para que en el caso de Mario Costeja fuera efectiva la aplicación del derecho al olvido, habría que haber borrado los archivos originales desde el servidor del diario *La Vanguardia*.

En el caso de la *web* 1.0, los problemas se generan porque la capacidad actual de los servidores, junto con el uso de CMS (*Content Management Sistem*), hacen que sea innecesario y hasta poco práctico borrar un contenido después de que es reemplazado por uno más nuevo. Esa es la razón por la cual el archivo queda —en los tiempos de la web— prácticamente por toda la eternidad.

La forma de recuperar una noticia, artículo, fotografía o video, es a través de la utilización de un buscador o motor de búsqueda. Esa es la razón por la cual el Tribunal de Justicia de la Unión Europea ordenó a Google borrar el artículo en el que aparecía nombrado Mario Costeja, desde su base de datos. El problema es que la solución no solo produjo el efecto Streisand, sino que pecó al no borrar el artículo desde el diario *La Vanguardia* y no considerar que Google no es el único buscador.

No obstante, el fallo del Tribunal de Justicia de la Unión Europea tiene cierta lógica, en un estado de desarrollo embrionario,

al considerar a los motores de búsqueda. Aunque para que se pueda aplicar de manera efectiva el derecho al olvido, es necesario considerar la forma en que los buscadores indexan la información proveniente de la *web* 1.0 y las redes sociales.

Si tratamos de ser lo más esquemático posible, un buscador tiene tres componentes básicos: la araña (*spider*), base de datos y *software* de búsqueda. La araña es un programa autónomo que posee inteligencia artificial, que recorre la *web*. Lo que ha hecho es leer una página, determinar cuál es el tema de ella, en función de las palabras que más se repiten y de las *metatags* (etiquetas de contenido) y enviar una copia de ella a su servidor. A continuación, entra a todos los *links* que están en la página y repite todo el proceso.

Cuando el servidor recibe la copia de la página *web*, la almacena en una base de datos y la cataloga de acuerdo con la definición de tema, tomada por la araña. El último proceso es de búsqueda por parte del usuario. Lo que interviene es el programa de búsqueda, que toma las palabras puestas por el usuario y va a buscar a la base de datos las coincidencias más cercanas y, de esa manera, entrega los resultados.

Las consecuencias que tiene el proceso de indexación para la aplicación del derecho al olvido son múltiples. La primera de ellas es que los motores de búsqueda hacen que cualquier contenido sea accesible para los usuarios de internet, pese a que se haya publicado hace más de diez años. Eso es lo central, porque permite recuperar un artículo dentro de un mar de contenidos en pocos segundos.

Cabe señalar que las arañas de los buscadores realizan el proceso de indexación de manera autónoma a todos los contenidos que puedan ingresar a través de *links*. Los únicos contenidos que no entran en este proceso son aquellos que están encriptados (protegidos por clave) o que están protegidos bajo el estándar de exclusión de robots (SRE, por sus siglas en inglés). El SRE es un acuerdo de ético tomado por los principales motores de búsqueda que le indica con toda claridad a la araña cuáles son los directorios dentro del servidor de alojamiento de páginas *web* que están protegidos, por lo que no pueden ser indexados.

Este punto es importante porque genera la oportunidad para que se aplique el derecho al olvido en aquellos casos en que está totalmente justificado, como en el de los menores de edad. Pese a que la implementación del SRE es bastante sencilla porque implica la creación de un archivo de texto (robots.txt) en el cual se indica cuáles son las carpetas dentro del servidor al cual no pueden ingresar los motores de búsqueda, esto debe ser implementado por los *webmasters* y archivar las informaciones en esos lugares del servidor. Ese ha sido el principal problema, por el alto grado de desconocimiento del tema y la dificultad que implica archivar fotografía, videos y documentos dentro de carpetas específicas.

El segundo aspecto es que los buscadores generan copias de todos los contenidos que indexan. Por lo que, pese a que algo se borre desde el servidor de alojamiento, sigue estando disponible desde la copia en caché, que es el nombre por el cual se conoce. Por lo tanto, si quisiéramos aplicar el derecho al olvido, debiéramos borrar los archivos desde el servidor de alojamiento y las copias caché de los distintos motores de búsqueda, más allá de Google.

Pese a que pudiéramos hacer eso, nada nos asegura que ocurra la existencia de lo que se denomina como servidores espejo. Es decir, que se hagan copias de los archivos y se suban a otros servidores, y que sean indexados nuevamente por los buscadores. Esa es la razón por la que pese a que Google borró de su base de datos el archivo en el cual se anunciaba el remate de los bienes de Mario Costeja, ahora tiene más de siete mil resultados en el mismo motor de búsqueda.

A ello hay que sumar que, en la práctica, las plataformas creadas por las redes sociales y las distintas aplicaciones diseñadas para los dispositivos móviles funcionan como servidores de alojamiento de contenidos. Es decir, cualquier persona puede subir a internet un archivo, sin la necesidad de contar con un servidor *host*, e inscribir un dominio. A ello hay que sumar que la API (interfaz de programación de aplicaciones) que utilizan las redes sociales están diseñadas para permitir la comunicación entre distintas aplicaciones, lo que se traduce en la facilidad para compartir contenidos entre usuarios y distintas plataformas, redes sociales o aplicaciones.

Cuando una persona comparte un video o una fotografía, se genera una copia en su dispositivo, en el servidor de la aplicación y la nube asociada. Es necesario aclarar que dependiendo del sistema operativo (IOSX o Android) y de las aplicaciones instaladas en un dispositivo móvil, se puede utilizar más de una nube que respalde de manera automática los fotografías, videos y páginas *web* consumidas o compartidas.

Un ejemplo de ello es que, si recibimos un meme a través de WhatsApp en un iPhone, se generarían copias en el dispositivo en el servidor de WhatsApp y en iCloud (nube de Apple). Y si a ello sumamos el uso de aplicaciones como Dropbox, tendríamos una nueva copia de la imagen en otra nube. Todo ello sin considerar la posibilidad de compartir el meme en Twitter y Facebook, lo cual suma dos servidores más, con las respectivas nubes asociadas a los dispositivos de los usuarios que visualicen el archivo.

A todas estas copias hay que agregar a los motores de búsqueda y los mercados de datos. Al interactuar por redes sociales como Facebook, muchas personas ignoran que las configuraciones de privacidad de esa red social permiten, por defecto, la indexación de los perfiles y los muros por parte de los buscadores. Como resultado de ello, todas las fotos subidas en Facebook también van a estar disponibles en la *web*, desde las copias en caché.

Los mercados de datos, según Craig y Ludloff (2011), son plataformas como Gnip a las que pueden acceder las empresas, instituciones, gobiernos y medios de comunicación previo pago, para utilizar la información almacenada en la nube. Pueden obtener desde información estadística, como estudios de mercado y comportamiento en línea de los usuarios, hasta perfiles de gustos de personas específicas, con nombre y apellido. Los mercados de datos lo que hacen principalmente es almacenar datos y metadatos provenientes de la *web* 1.0 y 2.0, con fines de investigación. Los mercados de datos proporcionan la información para realizar los análisis propios del big data. La diferencia fundamental con los buscadores es que el acceso a la información almacenada por ellos es previo pago, se

centra principalmente en los contenidos de las redes sociales y, junto con los datos, se almacenan todos los metadatos asociados.

Previo al análisis de los motivos y posibilidad de aplicar el derecho al olvido entre tres ecosistemas digitales, es necesario volver brevemente a las arquitecturas de control, en los términos de Lessig.

Web, app y big data

La aplicación del derecho al olvido en internet está directamente asociada a las arquitecturas de control de las que habla Lessig. Pese a que en la actualidad es posible rastrear los números IP y, por lo tanto, identificar a los usuarios, la *web* 1.0 tiene una arquitectura que se caracteriza por ser más libre, en cuanto a la publicación de contenidos. Aunque sea posible rastrear la fuente, no existen controles que impidan la publicación.

Además, hay que considerar que los sistemas de filtrado de contenidos han demostrado altos niveles de ineficacia, debido a que es posible vulnerarlos al cambiar las etiquetas (*metatags*) de los contenidos. Un aspecto que es necesario recalcar es que en la *web* 1.0, los grados de control están acentuados en el usuario (receptor) y no en el emisor. En el caso de la *web* 2.0, tenemos un ecosistema que apunta cada vez más hacia las arquitecturas de control, pese a que se proyecte una apariencia contraria, en la cual las personas piensan que el anonimato está garantizado. En este punto debemos detenernos brevemente en un aspecto de corte tecnológico, que tiene connotaciones directas sobre las arquitecturas de control.

Aunque las primeras redes sociales como MySpace y Facebook nacieron bajo entornos web, en la actualidad la mayoría de ellas funcionan bajo el esquema de aplicaciones (apps). Tal como lo explicó Isaacson (2011), quien realizó la biografía de Steve Jobs, las *apps* permiten crear una plataforma que es abierta en una forma bastante controlada, que les permite a desarrolladores externos crear *softwares* y contenido, como si se tratara de un jardín comunitario estrictamente curado y enrejado.

Para entender esta afirmación, es necesario señalar que cuando Jobs creó el primer dispositivo móvil, el iPod, desarrolló un nuevo modelo de negocios que le permitiera mantener un mayor nivel de control. Tal como lo dijimos anteriormente, la *web* carece de un control central, porque cualquier persona puede conectarse, subir contenidos y desarrollar aplicaciones para ella, siempre y cuando respete los protocolos de comunicación.

Los dispositivos móviles, como los teléfonos inteligentes y tabletas, funcionan bajo el esquema de aplicaciones o *apps*, en donde sí existe un control central. Todas ellas deben ser confeccionadas exclusivamente con el *kit* de desarrollo proporcionado por la empresa que creó el sistema operativo del dispositivo móvil. Además, existe un nodo central desde el cual deben ser descargadas las *apps*. Nos referimos a la App Store de Apple (IOSX) y Google Play (Android).

Por lo tanto, toda aplicación debe estar confeccionada en el lenguaje propio de cada sistema operativo y solo puede ser distribuida desde la tienda oficial de Apple y Google. Si partimos de la base de que el código es ley, quien la define en este ecosistema digital son las dos principales empresas tecnológicas: Apple y Google. Ellos son quienes definen si alguna aplicación se puede publicar o no.

A pesar de que en el mundo de las redes sociales existe la sensación de altos grados de libertad para publicar contenidos, hay mecanismos de control que permitirían aplicar el derecho al olvido en el mundo de las redes sociales basadas en el ecosistema de las *apps*. Un ejemplo de ello es centro de denuncias de Facebook[1].

Si hacemos una revisión de las principales redes sociales (YouTube, Facebook, Twitter, Fickr, Instagram o Pinterest), todas tiene mecanismos de denuncias que permiten eliminar contenidos que son considerados ofensivos, que hacen apología del odio racial o vulneran los derechos de autor.

A diferencia de lo que sucede en la *web* 1.0, toda la publicación de contenidos en las redes sociales se hace cuando el usuario está *logueado*. Eso significa que, para subir un video o imagen, debe haber creado una cuenta previamente, por lo que se puede geolocalizar a esa

1 https://es-es.facebook.com/help/181495968648557/.

persona y asociar su cuenta con una dirección IP y con un dispositivo móvil o computador. Un simple experimento para comprobar lo anterior es el siguiente. La próxima vez que viaje al extranjero pida prestado un computador e intente ingresar desde allí a su cuenta de Facebook o Gmail. Lo más probable es que no pueda hacerlo, porque el servidor leerá ese ingreso como un intento de *hackeo*, porque el computador, la IP y los datos de geolocalización no coinciden con sus comportamientos habituales. El servidor interpretará el hecho como el intento de una persona en otro país, con otro computador y otra IP, de acceder a su cuenta.

Para efectos de la aplicación del derecho a la información, eso significa que una red social puede eliminar y filtrar desde su servidor ciertos contenidos. En este punto es necesario que nos detengamos brevemente porque no es lo mismo ética y técnicamente, filtrar y eliminar. Por eliminar debemos entender como el borrado de un archivo desde un servidor porque se considera que es injurioso, ofensivo, promueve el odio racial o comete apología de la violencia y el terrorismo.

El filtrado es distinto, porque es similar a la aplicación de la censura en los medios de comunicación tradicionales. Es un sistema que reconoce una firma digital, etiqueta de contenido (*metatag*) o dirección IP, e impide que el contenido sea publicado en una red social. Un nuevo experimento para comprobar la existencia de los sistemas de filtrado sería digitalizar un pequeño segmento de cualquier película de la saga de *Star Wars* y tratar de subirlo a YouTube. Antes de que se publique el video, una advertencia del sistema señala que se está intentando subir un contenido que atenta contra los derechos de autor y que, de publicarse, se podría eliminar la cuenta del usuario.

A diferencia del sistema de denuncia que elimina un contenido, después de un análisis por parte del personal de la red social, el sistema de filtrado es en sí una medida de censura porque es previa a la publicación.

No obstante, la existencia de los sistemas de filtrado en las redes sociales nos lleva a un nuevo plano: el de los metadatos. A

diferencia de la web 1.0, en la 2.0 y 3.0 los metadatos adquieren una importancia central a la hora de analizar el derecho al olvido.

Gran parte de las denuncias que hacen los usuarios de las redes sociales se deben a fotografías ofensivas que son subidas por terceros y que son etiquetadas (*tagueadas*) con su nombre. La etiqueta es un metadato que se le agrega a una imagen o video, que permite asociarla con una persona o un perfil específico dentro de la red social. Es necesario recordar que Facebook posee un *software* de reconocimiento facial, que etiqueta de manera automática las fotografías que son subidas por los usuarios.

La importancia que radica en este punto es que crea una diferencia entre el derecho al olvido de los contenidos (1.0) y de los metadatos (2.0 y 3.0). Es muy diferente borrar un video o fotografía, con todas las implicaciones éticas que ello tiene, que limitar el etiquetado para asociarlo a un perfil o identidad específicos.

En gran parte de los casos en que personas comunes denuncian una imagen dentro de las redes sociales por considerarla ofensiva o injuriosa hacia ellos, el problema tiene su origen en el etiquetado automático o que es realizado por una tercera persona. Al no existir una etiqueta que diga que ha sido subida una fotografía de alguien, que lo coloque dentro del muro de sus contactos y lo informe dentro de las notificaciones del sistema operativo de la tableta o el teléfono inteligente de los contactos de esa persona, la imagen pasará desapercibida.

De acuerdo con lo que plantean Scoble e Israel (2014), la etiqueta cumple una función contextual porque relaciona a la persona y el contenido de la etiqueta con su ecosistema social. Para poder entender esta afirmación, es necesario dar una breve mirada a la publicidad de carácter contextual que tienen las redes sociales. A diferencia de lo que sucede en las industrias culturales, la publicidad que le aparece a una persona en Facebook va a depender de su edad, sexo, ubicación geográfica, gustos, los sitios a los que le puso *like*, los videos y fotografías que vio, comentó, los perfiles que vio e, incluso, las actualizaciones que realizó en sus estados de ánimo dentro de su perfil. Por esa razón, la publicidad que se le despliega a un

adolescente chileno, hombre de veinte años, que estudia derecho y le gusta el hip hop, va a ser muy distinta de la compañera de curso que está sentada a su lado.

Lo que sucede es que lo 2.0 y lo 3.0 van de la mano en este caso, y están fuertemente ligados al big data y a la inteligencia artificial. A partir de los contenidos y la interacción con otras personas a través de las redes sociales, se generan metadatos, los cuales son procesados en tiempo real para brindarle contenidos y publicidad a la carta. Un ejemplo de ello son los algoritmos predictivos que utiliza Amazon para recomendar libros a los usuarios de su servicio Kindle. Se analizan los libros que compra una persona, los que lee, hasta qué página los lee, qué subraya, anota, comenta, los libros que busca y todo ello lo compara con otros usuarios que tienen un comportamiento similar, para recomendar posibles lecturas. Cabe señalar que, para realizar este artículo, gran parte de la bibliografía tiene su origen en «las recomendaciones para usted» que hace Kindle.

El tratamiento contextual que tiene la utilización de las etiquetas por parte de las redes sociales hace que para que se produzca un daño al honor o la vida privada de una persona, no sea necesario que un contenido sea *trending topic* o trascienda a los medios de comunicación masivos. Basta con que la etiqueta comunique la publicación de una fotografía ofensiva a veinte personas, que conforman su círculo social más cercano, para que se produzca el daño.

Por lo mismo, cuando pasamos al nivel 2.0 y 3.0, es necesario que hablemos del derecho al olvido del dato y el metadato. La sola limitación del etiquetado puede eliminar gran parte de los problemas porque evita que otros usuarios se enteren de algo y recuperen la información a través de búsquedas.

El comportamiento contextual de las redes sociales reconfigura el sentido que el derecho al olvido tiene en los medios de comunicación tradicionales. Zittrain (2008) define el derecho al olvido como el derecho que tiene toda persona a declararse en bancarrota social para comenzar nuevamente. Sin embargo, cuando hablamos del derecho al olvido en los medios de comunicación tradicionales, siempre nos estamos refiriendo a hechos de connotación pública, que gracias a la

alarma que produjeron marcaron la agenda temática. Desde el punto de vista del derecho a la información y tal como señala Desantes (1993), son hechos que las personas deben conocer para votar de manera informada y, por lo tanto, libre.

En el caso de las redes sociales, eso no es siempre así. Si analizamos el tema de los memes, es muy distinto hablar del caso de corrupción cometido por un político, a la de una joven de diecinueve años de la ciudad de Curicó en Chile, en el que se publicó una fotografía suya, con una leyenda que decía: «Tengo cara de travesti» (LUN, 01.01.2015).

En el caso de la joven nos encontramos con una información que no es de interés público, que no afecta a la vida democrática del país, pero que le produjo un grave daño a su honra, porque la fotografía fue difundida en su círculo social. A partir de lo anterior, se configuran dos nuevas capas o niveles dentro del derecho al olvido que son de especial interés, porque afectan a personas comunes y corrientes, con informaciones que no son de interés público. Nos referimos al derecho al olvido contextual y de los metadatos.

Sensores, vestibles, big data y la internet de las cosas

Al hablar de la importancia que adquiere en la actualidad el derecho al olvido en los ecosistemas digitales, es necesario que, junto a las redes sociales, nos refiramos, aunque sea brevemente, al nuevo entorno generado por los sensores, vestibles, la internet de las cosas y el big data.

Si las redes sociales nos agregaban lo contextual y los metadatos al derecho al olvido, la web 3.0 produce un efecto multiplicador. Tanto los dispositivos móviles, como los vestibles, se caracterizan por tener sensores, que capturan datos y metadatos. La diferencia está en que los vestibles los capturan de una forma casi automática, lo que implica altos y bajos niveles de intrusión, dependiendo del punto de vista desde el cual se mire. La forma casi imperceptible en que los vestibles registran audio, video o funciones corporales como la presión sanguínea y el pulso, hace que el registro de los datos y

metadatos sea poco intrusivo. No obstante, los resultados son altamente intrusivos debido a la facilidad con la cual se pueden grabar y subir contenidos a la nube, en todo tipo de espacios y situaciones. Los vestibles al estar *logueados* en todo momento, basta con darles una orden verbal para que graben y otra, para que publiquen en un *blog* o una red social.

Cabe señalar que la realidad aumentada lleva el etiquetado a otro nivel, debido a que el simple acto de mirar cualquier objeto activa etiquetas con metadatos para advertir la ocurrencia de algo o señalar que hay un contenido asociado a ello. El simple acto de mirar una cara, puede activar un *software* de reconocimiento facial, que identifique a la persona y nos muestre su perfil en Facebook o las fotografías en las que está etiquetado.

Un aspecto que debemos recordar es que la mayor parte de las tecnologías de carácter contextual están basadas en el uso de los metadatos para predecir la conducta de las personas. Al hablar del big data y de la minería de datos entramos en una zona gris, que tiene bastantes matices, que dependen del tipo de datos recolectados, de quienes son los que recolectan y la finalidad para la cual se hace.

Si Amazon recolecta mis datos y metadatos asociados a la lectura de libros en Kindle, las búsquedas en Google y de navegación en su sitio y otros, para predecir mis preferencia de consumo y de esa manera ofrecerme productos que yo necesitaría, no se produciría un daño, ni a mi vida privada, ni a mi honor. Algo muy distinto sería que prestadores de salud recolectaran datos de funciones corporales obtenidos a través de los sensores de vestibles y eso lo cruzaran con el uso de la tarjeta de crédito, para decidir si a esa persona se le da a no, cobertura al momento de solicitarla frente a una enfermedad. Qué pasaría si autoridades de gobierno realizaran minería de datos a los comentarios políticos realizados en las redes sociales antes de seleccionar a las personas beneficiadas por programas sociales.

Al hablar del big data, el derecho al olvido adquiere un nuevo nivel, que Craig y Ludlof (2011) lo denominan como predictivo y que permite realizar acciones parecidas a las desarrolladas en la película *Minority Report*. En el caso de Mario Costeja, la razón

que lo motivó a ejercer su derecho al olvido en internet fue el daño a su honra que le produciría el que cada vez que alguien pusiera su nombre en Google apareciera un anuncio de remate de sus bienes. Cuando llevamos el derecho al olvido al nivel predictivo que tiene el big data, estamos hablando de un daño a la persona totalmente distinto. No es un daño a su honra, honor o vida privada.

El análisis de los comentarios realizados en redes sociales, los memes compartidos, junto con el historial de navegación de los usuarios a internet y todos los metadatos asociados a lo anterior, pueden revelar de manera precisa la postura política de las personas. Esa información puede ser usada para preferir a unos encima de otros, al momento de seleccionar a los beneficiados por políticas de asistencia estatal o para perseguir a la disidencia política. La aplicación del derecho al olvido al nivel del big data está más relacionado con el ámbito de las libertades personales y la discriminación, que con la esfera de la vida privada.

Asimismo, este es un ámbito en el cual la aplicación del derecho al olvido pasa más por un tratamiento ético por parte de los mercados de datos. Lo que se necesita es un compromiso bastante similar al que realizaron las empresas que desarrollan encuestas y estudios de mercado, al tratar la información a nivel estadístico y no identificar a las personas. De esta manera, se podría realizar todo tipo de análisis sin dañar a las personas.

Este es un aspecto que es necesario recalcar porque estamos a las puertas de una nueva revolución tecnológica: la internet de las cosas. Tal como lo explica Stephenson (2012), estamos en una nueva etapa histórica en la cual hay más cosas (teléfonos inteligentes, sensores industriales, electrodomésticos, autos) conectados a internet que personas. En la internet de las cosas los aparatos y dispositivos adquieren inteligencia, toman sus propias decisiones y se comunican entre sí, para cumplir sus tareas de manera autónoma.

Bajo la lógica de la internet de las cosas, los sensores de los vestibles, dispositivos móviles, vehículos y todos los objetos que tengan inteligencia artificial van a registrar datos y metadatos de manera automática, los cuales los almacenarán en la nube para realizar análisis

en tiempo real. Cuando nos referimos al derecho al olvido al nivel de la internet de las cosas, estamos hablando de la recopilación de información del comportamiento y las funciones corporales de las personas, lo cual pude utilizarse para predecir los estados de ánimo y los sentimientos de las personas, a través del uso de la inteligencia artificial. Claramente estamos frente a un nivel altamente intrusivo en la intimidad de las personas, y que es posible de ser realizado sin el más mínimo consentimiento y conocimiento de las mismas.

Pese a que esto pueda parecer un tanto distópico, la inteligencia artificial y la internet de las cosas han ido tomando el control de distintos procesos sociales de manera acelerada. Ciudades como Río de Janeiro y Nueva York ya utilizan sistemas de gestión que aplican los principios de la internet de las cosas, para tomar decisiones de manera predictiva y adelantarse a los hechos.

Tanto Google como BMW están trabajando en automóviles autónomos que utilizan la internet de las cosas como plataforma básica de funcionamiento. Lo que sucede es que, para la mayor parte de las personas, este tipo de tecnologías es invisible porque funcionan en un nivel muy cotidiano y se han hecho tan presentes en sus vidas, que ya no es posible observarlas.

Al hablar del big data y la internet de las cosas, llevamos el derecho al olvido a un plano nuevo, que no se relaciona con los medios de comunicación y la protección del honor o la honra de las personas. Nos estamos moviendo en una dimensión que afecta más la capacidad para tomar decisiones de manera libre y de no ser discriminado por lo que sucede al interior de nuestros cuerpos y mente.

El derecho al olvido en los ecosistemas digitales

A partir de lo que hemos analizado con anterioridad, surge la necesidad de hacer una clara diferenciación de lo que sucede en cada ecosistema digital antes de aplicar el derecho al olvido, para que no pase lo mismo que en el caso de Mario Costeja.

En el ecosistema 1.0 nos referimos a informaciones publicadas por sitios *web* y que son indexadas por motores de búsqueda, como

Google. Esto es importante porque desde el punto de vista ético, estamos situados en un nivel donde la publicación de contenidos es realizada por profesionales (periodistas y medios de comunicación electrónicos) o semiprofesionales (blogueros), y la indexación, por las industrias tecnológicas (buscadores).

Es necesario hacer esta diferenciación, por las implicancias que tiene para la aplicación del derecho al olvido en dicho ecosistema. La publicación de contenidos en la *web* 1.0 es un proceso manual, por lo que la aplicación del derecho al olvido pasa por un proceso de toma de decisiones de carácter editorial. Mientras que la indexación es automática y está marcada por la inteligencia artificial de las arañas de los motores de búsqueda.

Ese un aspecto por considerar porque pone de manifiesto la inutilidad de la solución establecida por el Tribunal de Justicia de la Unión Europea para garantizar el derecho al olvido del ciudadano español. El hecho de borrar a una persona desde la base de datos de un motor de búsqueda no asegura la aplicación del derecho al olvido porque la araña seguirá indexando nuevas páginas, con nuevos resultados. Mientras no se borren los contenidos desde los servidores donde se publicaron, no se podrá aplicar el derecho al olvido.

El SRE (*Standard for Robot Exclusion*) surge como una alternativa para limitar la indexación de páginas *web* por parte de los buscadores, pero no es una alternativa real debido a que su implementación depende de los *webmasters* de los sitios. El alto grado de desconocimiento de dicho acuerdo, sumado a su baja utilización, hacen que sea poco realista su utilización.

Por lo tanto, la única forma de ejercer el derecho al olvido de manera correcta sería bajar el archivo desde el sitio que publicó el contenido y solicitar que se borre la copia caché del buscador. La aplicación de otro tipo de medidas en los motores de búsqueda podría configurar sistemas de censura, que afectarían a la información futura.

Tal como lo señala Castellanos (2013), el derecho al olvido, desde el punto de vista conceptual, tiene dos vertientes que es necesario considerar. Una que está referida a la protección de datos personales y la otra es «un derecho a equivocarse y volver a empezar». La

aplicación del derecho al olvido por parte del Tribunal de Justicia de la Unión Europea conserva el sentido de ambas vertientes, pero en ningún caso puede aplicarse a nueva información.

Desde el punto de vista técnico, sería posible aplicar el derecho al olvido a los metadatos (etiquetas) asociadas a un contenido que esté en la *web*. Eso significaría que la araña del motor de búsqueda no podría indexar y publicar en la base de datos una etiqueta de contenido, para que al ingresar los términos de búsqueda nadie los pueda encontrar. Desde el punto de vista del derecho a la información, eso constituiría una medida de censura porque impediría que las personas accedieran a información nueva, recién publicada.

El autor afirma que el derecho al olvido es la «facultad de evitar que terceros recuerden hechos del pasado veraces y que en su día revistieron una notoriedad pública que con el paso del tiempo pereció». Este punto es central, porque la aplicación del derecho al nivel del metadato impediría la indexación de contenidos nuevos.

Cabe señalar que es difícil aplicar el derecho al olvido en la web 1.0 sin caer en la censura. Es por esa razón que este problema debe ser tratado a nivel ético por parte de periodistas, editores, blogueros y *webmasters*. La solución establecida al pensar que depende de un buscador como Google carece de sentido práctico, ya que a los pocos días encontraremos aún más resultados que antes.

Consideraciones finales

El derecho al olvido en las redes sociales y las *apps* (aplicaciones) nos plantea nuevos desafíos. Tal como lo señala Castellanos, este debe aplicarse cuando una información pierde su interés público. Sin embargo, la mayor parte de los problemas relativos al honor y la honra de las personas en las redes sociales son a un nivel contextual, lo que significa que son informaciones que no tienen interés público. Son fotografías, videos o comentarios que dañan la honra, el honor, o acosan a personas comunes y corrientes.

Debido a que se trata de la eliminación de contenidos que no tienen interés público, los mecanismos de control y denuncia que han

implementado las redes sociales no plantean ningún peligro para el derecho a la información en los entornos digitales. Eso sí, la principal dificultad está en los tiempos de respuesta y en la facilidad para generar copias de los contenidos a nivel local (dispositivo), nube o en otras redes sociales, lo que en la práctica anula gran parte de la utilidad de los mecanismo de control.

Por lo mismo, la limitación del etiquetado de personas en el caso de fotografías y videos es una medida necesaria, que a diferencia de lo que sucede en la *web* 1.0 no constituye una medida de censura. En primer lugar, porque no impide la publicación y no se trata de contenidos de interés público.

En materia de big data y la internet de las cosas, la aplicación del derecho al olvido se convierte en una necesidad debido a que el análisis de los mensajes y de los metadatos asociados a ellos ya no se refiere al honor, honra o vida privada, sino que el hecho de poder predecir la conducta de las personas puede utilizarse con fines políticos, religiosos o de toda índole, para controlar la disidencia o el manejo de las opiniones personales. Es necesario, por tanto, que se limite la conexión de datos y metadatos corporales y conductuales recopilados por vestibles y objetos inteligentes, con la identidad de las personas, para evitar que las personas sean discriminadas por actores públicos o privados, en función de sus estados de salud, cultura, costumbres o creencias. Cabe señalar que este es un plano en el cual la aplicación técnica es posible y depende tanto de la disposición de la industria tecnológica como de los estados para legislar sobre este punto.

Bibliografía

Barlow, Mike (2013). *The culture of Big Data*. Cambridge: O'Reilly.

Boyd, Dann (2014). *It's Complicated: The Social Lives of Networked Teens*. New Haven: Yale University Press.

Castellano, Pere (2013). El carácter relativo del derecho al olvido en la red y su relación con otros derechos, garantías e intereses legítimos. En Loreto Corredoira y Lorenzo Cotino, Lorenzo (eds.), *Libertad de expresión e información en Internet: Amenazas y protección de los derechos personales* (pp. 451-474). Madrid: Centro de Estudios Políticos y Constitucionales.

Castells, Manuel (2012). *Comunicación y poder*. México, D.F.: Siglo XXI Editores.

Craig, Terence; Ludloff, Mary (2011). *Privacy and Big Data*. Cambridge: O'Reilly.

Desantes Guanter, José María (1990). *Información y Derecho*. Santiago: Pontificia Universidad Católica de Chile.

Desantes, José María (1993). *La información como deber*. Buenos Aires: Colección de la Facultad de Ciencias de la Información de la Universidad Austral.

Isaacson, Walter (2011). *Steve Jobs*. New York: Simon & Schuster.

Lessig, Lawrence (2008). *The Code: Version 2.0*. New York: Basic Books.

Mc Luhan, Marshall (1962). *The Gutenberg Galaxy*. Toronto: University of Toronto Press.

Needham, Jeffrey (2013). *Disruptive possibilities: How Big Data changes everything*. Cambridge: O'Reilly.

O'Reilly Media Inc. (2012). *Big Data now*. Cambridge: O'Reilly.

Orza, Ramón (2013). El derecho al olvido en Internet: Algunos intentos para su regulación legal. En Loreto Corredoira y Lorenzo Cotino (eds.), *Libertad de expresión e información en Internet: Amenazas y protección de los derechos personales* (pp. 475-500). Madrid: Centro de Estudios Políticos y Constitucionales.

Payton, Theresa; Claypoole, Ted (2014). *Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family*. New York: Rowmand & Littlefield.

Rosen, Jeffrey (2012). The right to be forgotten. 64 STAN. L. REV. ONLINE 88 February 13.

Scoble, Robert; Israel, Shel (2014). *Age of Context: Mobile, Sensors, Data and the Future of Privacy*. Patrick Brester Press.

Stephenson, David (2012). *SmartStuff: an introduction to the Internet of Things*. Amazon.

Weber, Rolf (2011). The right to be forgotten: More than a Pandora's Box? *JIPITEC* 120.

Zittrain, Jonathan (2008). The Future of the Internet: And How to Stop It. New Haven: Yale University Press.

Sentencias:

Tribunal de Justicia de la Unión Europea, Sentencia en el asunto C-131/12 Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González. Sentencia del 13 de mayo de 2014. Disponible en: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES.

La revaloración de la identidad digital, ¿se puede «recomenzar» en la red 3.0? Aspectos legales y sociales

María Teresa Nicolás Gavilán

Introducción

Con la llegada de las redes sociales y del internet 3.0, la comunicación se ha multiplicado de un modo exponencial. En la sociedad de la información los usuarios de las redes intercambian, de modo voluntario e involuntario, datos de voz, de imagen, etc. Internet es un repositorio inmenso de datos personales y colectivos compartidos por los propios interesados o por terceros. Además, la aceleración en la comunicación reduce el tiempo para la reflexión, interconexión e inmediatez son los componentes principales del ecosistema mediático.

Este nuevo escenario comunicativo trae consigo nuevas responsabilidades para los actores del proceso: los internautas son los responsables de los contenidos que comparten —propio o ajeno—, las plataformas digitales deben garantizar un doble derecho: la información y la privacidad, y la autoridad tiene que velar que estos derechos se cumplan, todo en un entorno virtual interconectado.

Para la legislación —que siempre sigue a la práctica, como dice el aforismo latino: *Da mihi factum, dabo tibi ius*—, la protección de las personas al amparo de la ley consiste en reconocer un derecho y dotarlo de protección legal, de ahí surge el llamado derecho al olvido. Una tutela jurídica que busca proteger dos bienes: el honor